IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application:	:	Group Art Unit: 2436
James P. Goddard	:	Examiner: Daniel L. Hoang
Serial No.: 10/690,017	:	IBM Corporation
Filed: 10/21/2003	:	Intellectual Property Law
Confirmation No.: 4833	:	Department SHBC/040-3
Title: SYSTEM, METHOD AND PROGRAM	:	1701 North Street
PRODUCT TO DETERMINE SECURITY	:	Endicott, NY 13760
RISK OF AN APPLICATION	:	

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

I. Real Party in Interest

International Business Machines Corporation is the real party in interest.

II. Related Appeals and Interferences

There are no related Appeals or Interferences.

III. Status of Claims

Claims 1-37 were previously canceled.

Claims 38-49 are pending, Finally Rejected and Appealed.

IV. Status of Amendments

An Amendment after Final Rejection was filed on December 5, 2011.

V. Summary of Claimed Subject Matter

Support for the claim elements is indicated in plain brackets [ ].

Claim 38 recites a computer program product for evaluating a security risk of an application. [Computer program implementing automated processes 200 and 300. Page 6 lines 1-13. Page 7 lines 19-28. Page 2 at end of line 18 - addition to end of original Summary by Amendment of November 22, 2011 copying original program product claims 21 and 24 to end of original Summary.] The computer program product includes one or more computer-readable tangible storage devices and program instructions stored on at least one of the one or more storage devices. [Page 6 lines 2-3. Flowchart of Figure 2 including steps 201-242. Step 308 of Flowchart of Figure 3. Page 2 at end of line 18, i.e. addition to end of original Summary by Amendment of November 22, 2011 copying original program product claims 21 and 24 to end of original Summary.] Program instructions determine whether employees of two or more customer corporations are authorized to concurrently share use of the application. [Decision 308 of Figure 3. Page 8 lines 16-17. Addition to end of original Summary by Amendment of November 22, 2011 copying original program product claims 21 and 24 to end of original Summary.] Program instructions determine whether a vulnerability in the application can be exploited by a user which has not been authenticated to the application. [Steps 240 and 242. Page 7 lines 15-18.] Program instructions assign numerical weights to the respective determinations. [Steps 310, 226, 215 and 222. Page 7 lines 6-15. Page 8 lines 17-18.] Each of the numerical weights corresponds to a significance of the respective determination in quantifying the security risk. [Page 2 lines 7-10 and 16-18. Addition to end of original Summary by Amendment of November 22, 2011 copying original program product claims 21 and 24 to end of original Summary.] Program instructions combine the numerical weights to quantify the security risk. [Page 4 lines 6-10. Steps 204, 242, 310 and 320. Page 6 line 14 to Page 7 line 18. Page 8 lines 13-21.] Program instructions compare the quantification of the security risk based on the combined numerical weights to a monetary value of a benefit of the application, and based on the comparison, recommend whether to certify the application for use. [Step 500. Page 10 line 28 to Page 11 line 7. Page 11 line 8 to Page 12 line 3.]

Claim 44 recites a system for evaluating a security risk of an application. [Computer with program instructions implementing automated processes 200 and 300. Page 6 lines 1-13. Page 7 lines 19-28. "Systems" of page 2 lines 2-18. Page 2 at end of line 18 - addition to end of original Summary by Amendment of November 22, 2011 copying original program product claims 21 and 24 to end of original Summary.] The computer system includes one or more processors, one or more computer-readable memories, one or more computer-readable tangible storage devices, and program instructions stored on at least one of the one or more storage devices for execution by at least one of the one or more processors via at least one of the one or more memories. ["Systems" of page 2 lines 2-18. Page 6 lines 2-3. Flowchart of Figure 2 including steps 201-242. Step 308 of Flowchart of Figure 3. Page 2 at end of line 18, i.e. addition to end of original Summary by Amendment of November 22, 2011 copying original program product claims 21 and 24 to end of original Summary.] Program instructions determine whether employees of two or more customer corporations are authorized to concurrently share use of the application. [Decision 308 of Figure 3. Page 8 lines 16-17. Addition to end of original Summary by Amendment of November 22, 2011 copying original program product claims 21 and 24 to end of original Summary.] Program instructions determine whether a vulnerability in the application can be exploited by a user which has not been authenticated to the application. [Steps 240 and 242. Page 7 lines 15-18.] Program instructions assign numerical weights to the respective determinations. [Steps 310, 226, 215 and 222. Page 7 lines 6-15. Page 8 lines 17-18.] Each of the numerical weights corresponds to a significance of the respective determination in quantifying the security risk. [Page 2 lines 7-10 and 16-18. Addition to end of original Summary by Amendment of November 22, 2011 copying original program product claims 21 and 24 to end of original Summary.] Program instructions combine the numerical weights to quantify the security risk. [Page 4 lines 6-10. Steps 204, 242, 310 and 320. Page 6 line 14 to Page 7 line 18. Page 8 lines 13-21.] Program instructions compare the quantification of the security risk based on the combined numerical weights to a monetary value of a benefit of the application, and based on the comparison, recommend whether to certify the application for use. [Step 500. Page 10 line 28 to Page 11 line 7. Page 11 line 8 to Page 12 line 3.]

VI. Grounds of Rejection to be Reviewed upon Appeal

Claims 38-49 were rejected under 35 USC 103(a) based on US 7,552,480 to Voss and US Publication 2001/0044737 by Halligan.

VII. Argument

General Caselaw on 35 USC 102 and 103

A claim cannot be anticipated under 35 USC 102 unless each and every element as recited in the claim is found in a single prior art reference. Richardson v. Suzuki Motor Co., 868 F.2d 1226, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

A claim cannot be obvious under 35 USC 103 unless (a) there is a reason that a person of ordinary skill in the art would have combined the references, and (b) all the claim elements are taught or suggested by the prior art. See In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438, 1443 (Fed Cir. 1991) and KSR Int'l Co. v. Teleflex, Inc., No. 04-1350 (USSC 30 April 2007). Otherwise, there is not a prima facie case of obviousness.

The Examiner bears the burden of establishing a prima facie case of obviousness based on prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992). Only if that burden is met, does the burden of coming forward with evidence or argument shift to the applicant. *Id.* All words in a claim must be considered in judging the patentability of that claim against the prior art." MPEP 2143.03; *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). If the examiner fails to establish a prima facie case, the rejection is improper and will be overturned. *In re Fine*, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). In the absence of a proper *prima facie* case of obviousness, an applicant who complies with the other statutory requirements is entitled to a patent. *See In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992).

"In order to rely on a reference as a bass for rejection of an applicant's invention, the reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker 977 F.2d 1443, 1446, 24 USCPQ2d 1443, 1445 (Fed. Cir. 1992).

Rejection of Claims 38-49 under 35 USC 103(a)
Based on US 7,552,480 to Voss and US Publication 2001/0044737 by Halligan

Claim 38 recites:

"program instructions to determine whether employees of two or more customer corporations are authorized to concurrently share use of the application;

program instructions to determine whether a vulnerability in the application can be exploited by a user which has not been authenticated to the application;

program instructions to assign numerical weights to the respective determinations, each of the numerical weights corresponding to a significance of the respective determination in quantifying the security risk;

program instructions to combine the numerical weights to quantify the security risk; and

program instructions to compare the quantification of the security risk based on the combined numerical weights to a monetary value of a benefit of the application, and based on the comparison, recommend whether to certify the application for use."

Voss assesses a security risk based on (a) threat of attack based on possible "threat agents", (b) possible mode of access to a computer system, and (c) privilege components of one or more vulnerabilities to a computer system. The possible "threat agents" are casual users, kiddy scriptors, hackers, disgruntled employees, legitimate consumers, competitors, political activists, agents of organized crime, law enforcement agents, or government agents. The possible modes of access include wide area network access, global network access, wireless

access, proprietary network access, packet switched network access, terminal access, and physical access. More specifically, Voss teaches:

> "It is a feature and advantage of the present invention to provide a method and system for assessing and **quantifying the risk exposure of an information system or application using a one-dimensional quantitative risk assessment model having applicability on several areas including, for example, assessment and policy enforcement**." (emphasis added) Voss Column 3 lines 15-20.

> "A numerical value is established for one or more threats of attack on an information system asset of the entity based on expert knowledge without reference to actuarial data. Likewise, based on expert knowledge without reference to actuarial data, **a numerical value is established for each of one or more access and privilege components of one or more vulnerabilities to attack on the information system asset.** Based upon the numerical values for threat and the access and privilege components for vulnerability so established, a security risk level for the information system asset can be computed.

An aspect of establishing the numerical value for the threat of attack involves establishing the potential for an attack on the information system asset by a threat agent based, for example, on a combination of motivation and ability of the threat agent for the attack. Possible threat agents can be identified by either or both of a business manager or an information security officer for the entity and include, for example, casual users, kiddy scriptors, hackers, disgruntled employees, legitimate consumers, competitors, political activists, agents of organized crime, law enforcement agents, or government agents. An aspect of establishing the numerical value for the access component of the vulnerability to attack involves, for example, identifying one or more modes of access required for an attack on the information system asset by the threat agent and/or one or more methods of attack available to the threat agent. **Possible modes of access can be identified by either or both of an information security officer or a technician for the entity and include, for example, wide area network access, global network access, wireless access, proprietary network access, packet switched network access, terminal access, or physical access. An aspect of establishing the numerical value for the privilege component of the vulnerability to attack involves, for example, identifying one or more unauthorized privileges that can be acquired by a threat agent from attack on the information system asset. Possible unauthorized privileges can likewise be identified by either or both of an information security officer or a technician for the entity and include, for example, super user privileges, security administrator privileges, super user read privileges, security auditor privileges, normal user privileges, or guest privileges.**

The security risk level for the information system asset is calculated as the product of the numerical value of the threat of attack times the numerical value for the access component of the vulnerability to attack times the numerical value for the privilege component of the vulnerability to attack on the information system asset. The security risk level so calculated can be used, for example, for comparison to a security risk level calculated for another information system asset. Further, a numerical value for a security risk level threshold limit for the information system asset can be established and a security policy implemented which mandates that if the security risk level calculated for the information system asset exceeds the prescribed security risk level threshold limit, remediation shall be initiated." (emphasis added) Voss Column 4 lines 10-66.

"An aspect of the present invention defines vulnerability in terms, for example, of privileges and access. When someone exploits a vulnerability, it results in their having privileges in addition to those which they would normally have. **A normal user may be able to access certain data from a computer, but if that person were to exploit a vulnerability, he or she might have additional control, for example, to see and/or delete other persons' data that he or she would not otherwise have. Thus, vulnerability has a component of which privilege is a major part.** The other component of vulnerability is defined according to this aspect in terms of the access that is necessary for a person to have in order to exploit the vulnerability, such as whether the vulnerability presents itself to the external environment, for example, via a network or a keyboard or mouse input, or requires access for the attacking entity to the physical box itself by its floppy disc drive." (emphasis added) Voss Column 7 line 66 to Column 8 line 14.

Claim 38 recites program instructions to determine whether employees of two or more customer corporations are authorized to concurrently share use of the application and program instructions to determine whether a vulnerability in the application can be exploited by a user which has not been authenticated to the application. Program instructions assign numerical weights to the respective determinations, each of the numerical weights corresponding to a significance of the respective determination in quantifying the security risk. Program instructions combine the numerical weights to quantify the security risk. Program instructions compare the quantification of the security risk based on the combined numerical weights to a monetary value of a benefit of the application, and based on the comparison, recommend whether to certify the application for use.

None of these features of claim 38 is taught or suggested by Voss. Voss assesses a security risk based on (a) threat of attack based on possible "threat agents", (b) possible mode of access to a computer system, and (c) privilege components of one or more vulnerabilities to a computer system. The possible "threat agents" are casual users, kiddy scriptors, hackers, disgruntled employees, legitimate consumers, competitors, political activists, agents of organized crime, law enforcement agents, or government agents. The possible modes of access include wide area network access, global network access, wireless access, proprietary network access,

packet switched network access, terminal access, and physical access. But, these teachings of Voss do not disclose or suggest any of the features of new claim 38 let alone the combination of features of claim 38.

The Examiner cited from Voss, "quantifying the risk exposure of an information system or application using a one-dimensional quantitative risk assessment model having applicability on several areas including, for example, assessment and policy enforcement". But, this is a high level statement of the objective **without the implementation of claim 38**.

The Examiner also cited from Voss, "establishing the numerical value for the threat of attack involves establishing the potential for an attack on the information system asset by a threat agent based, for example, on a combination of motivation and ability of the threat agent for the attack. Possible threat agents can be identified by either or both of a business manager or an information security officer for the entity and include, for example, casual users, kiddy scriptors, hackers, disgruntled employees, legitimate consumers, competitors". But, this is another high level statement of something to consider, i.e. the potential for an attack is based on a combination of motivation and ability of the threat agent, **without the implementation of claim 38.**

The Examiner also cited from Voss, "An aspect of establishing the numerical value for the privilege component of the vulnerability to attack involves, for example, identifying one or more **unauthorized privileges** that can be acquired by a threat agent from attack on the information system asset. Possible unauthorized privileges can likewise be identified by either or both of an information security officer or a technician for the entity and include, for example, **super user privileges, security administrator privileges, super user read privileges, security auditor privileges, normal user privileges, or guest privileges**". But, **these are not the specific risk factors recited in claim 38,** i.e. program instructions to determine whether employees of two or more customer corporations are authorized to concurrently share use of the application and program instructions to determine whether a vulnerability in the application can be exploited by a user which has not been authenticated to the application.

The Examiner also cited from Voss, "The security risk level so calculated can be used, for example, for comparison to a security risk level calculated for another information system asset. Further, a numerical value for a security risk level threshold limit for the information system asset can be established and a security policy implemented which mandates that if the security risk level calculated for the information system asset exceeds the prescribed security risk level threshold limit, remediation shall be initiated." While Voss indicates a numerical value for a security risk level, **Voss does not consider the specific risk factors or claim 38**. Therefore, the numerical algorithm of claim 38 for assessing risk is not taught or suggested by the numerical value for risk taught by Voss.

Also, as acknowledged by the Examiner, "Voss is mute in teaching comparing the quantified security risks with a monetary value of a benefit of the application." For this, the Examiner cited Halligan. However, Halligan does not fill this or the other noted gaps of Voss.

Halligan teaches a technique to determine the commercial value of a trade secret and the cost to protect the trade secret, and then compare the cost to the value to determine if the trade secret is worth the cost of the protection.

> "FIG. 6 provides a detailed flow diagram illustrating the analysis of trade secret value data by a value processor (VP) of the accounting system. The accounting system may perform an analysis to determine the net present value and net present value factor, for example on a 1 to 5 scale, of any trade secret in the accounting system. The net present value may be calculated from the **estimated commercial value of the trade secret** on a specified date, and a depreciation or appreciation method, using Generally Accepted Accounting Principles or other methods. The trade secrets may then be divided into groups by the accounting system, comprising in the example shown four quartiles of net present value for a 1 to 5 scale.

An additional calculation may be made from the security measures factor and the net present value factor to generate the **ratio of the security measures factor and the net present value factor for those trade secrets selected for analysis**. The accounting system may also identify outlying values of this ratio. These outlying values may represent trade secrets for which the security measures taken may not be justified by a low commercial value of the trade secret, which security measures may result in increased cost to the company, and trade secrets for which the security measures taken may be inadequate for the high commercial value of the trade secret, which inadequacy may result in risk of loss of the trade secret and resulting financial loss.

An additional calculation may be made from the economic benefit factor of a trade secret from Section 757 of the First Restatement of Torts and the net present value factor to generate the ratio of the economic benefit factor and the net present value factor for those trade secrets selected for analysis. The accounting system may also identify outlying values of this ratio. These outlying values may represent trade secrets for which the economic benefit factor and the net present value factor appear to be out of correspondence with each other. A trade secret with a high economic benefit factor should correspond with a high net present value factor and a trade secret with a low economic benefit factor should correspond with a low net present value factor." (emphasis added) Halligan Paragraphs [0119-0121]

Thus, Halligan teaches a technique to determine the commercial value of a trade secret and the cost to protect the trade secret, and then compare the cost to the value to determine if the trade secret is worth the cost of its protection. Firstly, note that the *protection cost* to trade secret value analysis of Halligan differs from the function of claim 38 which compares the *security risk* to the application value. Also, Halligan does not teach or suggest program instructions to determine whether employees of two or more customer corporations are authorized to concurrently share use of the application and program instructions to determine whether a vulnerability in the application can be exploited by a user which has not been authenticated to the application. Therefore, Halligan does not fill the foregoing gaps of Voss, and the combination of Voss and Halligan does not form a prima facie case of obviousness. Consequently, the rejection of claim 38 should be reversed.

Claims 39-43 depend on claim 38 and therefore, distinguish over Voss and Halligan for the same reasons that claim 38 distinguishes thereover.

Claims 44-49 distinguish over Voss and Halligan for the same reasons that claims 38-43 respectively, distinguish thereover,

Based on the foregoing, Appellants request reversal of all rejections made by the Examiner.

Respectfully submitted,

Dated: Dec. 6, 2011
Phone: 607-429-4368
Fax: 607-429-4119

/Arthur J. Samodovitz/
Arthur J. Samodovitz
Reg. No. 31,297

VIII. Claims Appendix

38. A computer program product for evaluating a security risk of an application, the computer program product comprising:

one or more computer-readable tangible storage devices and program instructions stored on at least one of the one or more storage devices, the program instructions comprising;

program instructions to determine whether employees of two or more customer corporations are authorized to concurrently share use of the application;

program instructions to determine whether a vulnerability in the application can be exploited by a user which has not been authenticated to the application;

program instructions to assign numerical weights to the respective determinations, each of the numerical weights corresponding to a significance of the respective determination in quantifying the security risk;

program instructions to combine the numerical weights to quantify the security risk; and

program instructions to compare the quantification of the security risk based on the combined numerical weights to a monetary value of a benefit of the application, and based on the comparison, recommend whether to certify the application for use.

39. The computer program product of claim 38 further comprising:

program instructions, stored on at least one of the one or more storage devices, to determine whether there is a requirement for authentication for user access to the application; and wherein

the program instructions to assign numerical weights to the respective determinations assign a numerical weight to the determination whether there is a requirement for authentication for user access to the application; and

the program instructions to combine the numerical weights to quantify the security risk also use the numerical weight for the determinations whether there is a requirement for authentication for user access to the application, in quantifying the security risk.

40. The computer program product of claim 38 further comprising:

program instructions, stored on at least one of the one or more storage devices, to determine whether a third party can obtain unauthorized administrative authority to data maintained by the application; and

program instructions, stored on at least one of the one or more storage devices, to determine whether a third party can obtain unauthorized read and/or write access to data maintained by the application; and wherein

the program instructions to assign numerical weights to the respective determinations assign a numerical weight to the determination whether a third party can have unauthorized administrative authority to data maintained by said application, and assign a numerical weight to the determination whether a third party can have unauthorized read and/or write access to data maintained by said application; and

the program instructions to combine the numerical weights to quantify the security risk also use the numerical weight for the determinations whether a third party can have unauthorized administrative authority to data maintained by said application and the numerical weight for the determination whether a third party can have unauthorized read and/or write access to the data, in quantifying the security risk.

41. The computer program product of claim 38 further comprising:

program instructions, stored on at least one of the one or more storage devices, to determine whether data accessible by a user via the application is confidential;

the program instructions to assign numerical weights to the respective determinations assign a numerical weight to the determination whether data accessible by a user via the application is confidential; and

the program instructions to combine the numerical weights to quantify the security risk also use the numerical weight for the determinations whether data accessible by a user via the application is confidential.

42. The computer program product of claim 38 wherein the monetary value of the benefit of the application is a cost savings due to use of the application.

43. The computer program product of claim 38 wherein the monetary value of the benefit of the application is a revenue gained by the application.

44. A system for evaluating a security risk of an application, the computer system comprising:

one or more processors, one or more computer-readable memories, one or more computer-readable tangible storage devices, and program instructions stored on at least one of the one or more storage devices for execution by at least one of the one or more processors via at least one of the one or more memories, the program instructions comprising:

program instructions to determine whether employees of two or more customer corporations are authorized to concurrently share use of the application;

program instructions to determine whether a vulnerability in the application can be exploited by a user which has not been authenticated to the application;

program instructions to assign numerical weights to the respective determinations, each of the numerical weights corresponding to a significance of the respective determination in quantifying the security risk;

program instructions to combine the numerical weights to quantify the security risk; and

program instructions to compare the quantification of the security risk based on the combined numerical weights to a monetary value of a benefit of the application, and based on the comparison, recommend whether to certify the application for use.

45. The computer system of claim 44 further comprising:

program instructions, stored on at least one of the one or more storage devices for execution by at least one of the one or more processors via at least one of the one or more memories, to determine whether there is a requirement for authentication for user access to the application; and wherein

the program instructions to assign numerical weights to the respective determinations assign a numerical weight to the determination whether there is a requirement for authentication for user access to the application; and

the program instructions to combine the numerical weights to quantify the security risk also use the numerical weight for the determinations whether there is a requirement for authentication for user access to the application, in quantifying the security risk.

46. The computer system of claim 44 further comprising:

program instructions, stored on at least one of the one or more storage devices for execution by at least one of the one or more processors via at least one of the one or more memories, to determine whether a third party can obtain unauthorized administrative authority to data maintained by the application; and

program instructions, stored on at least one of the one or more storage devices for execution by at least one of the one or more processors via at least one of the one or more memories, to determine whether a third party can obtain unauthorized read and/or write access to data maintained by the application; and wherein

the program instructions to assign numerical weights to the respective determinations assign a numerical weight to the determination whether a third party can have unauthorized administrative authority to data maintained by said application, and assign a numerical weight to the determination whether a third party can have unauthorized read and/or write access to data maintained by said application; and

the program instructions to combine the numerical weights to quantify the security risk also use the numerical weight for the determinations whether a third party can have unauthorized administrative authority to data maintained by said application and the numerical weight for the determination whether a third party can have unauthorized read and/or write access to the data, in quantifying the security risk.

47. The computer system of claim 44 further comprising:

program instructions, stored on at least one of the one or more storage devices for execution by at least one of the one or more processors via at least one of the one or more memories, to determine whether data accessible by a user via the application is confidential;

the program instructions to assign numerical weights to the respective determinations assign a numerical weight to the determination whether data accessible by a user via the application is confidential; and

the program instructions to combine the numerical weights to quantify the security risk also use the numerical weight for the determinations whether data accessible by a user via the application is confidential.

48. The computer system of claim 44 wherein the monetary value of the benefit of the application is a cost savings due to use of the application.

49. The computer system of claim 44 wherein the monetary value of the benefit of the application is a revenue gained by the application.

IX. Evidence Appendix

There is no evidence entered or relied upon in this Appeal.

X. Related Proceedings Appendix

There are no related Appeals or Interferences, and therefore, no copies of such decisions to attach.